

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

J1046 U.S. PTO  
10/080697  
02/25/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 8月28日

出 願 番 号

Application Number:

特願2001-257794

出 願 人

Applicant(s):

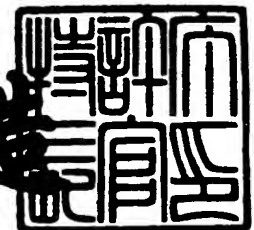
三菱電機株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 9月13日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 533298JP01

【提出日】 平成13年 8月28日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/00

【発明者】

    【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会  
社内

    【氏名】 前田 卓志

【発明者】

    【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会  
社内

    【氏名】 松下 雅仁

【発明者】

    【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会  
社内

    【氏名】 笹川 耕一

【特許出願人】

    【識別番号】 000006013

    【住所又は居所】 東京都千代田区丸の内二丁目2番3号

    【氏名又は名称】 三菱電機株式会社

【代理人】

    【識別番号】 100062144

    【弁理士】

    【氏名又は名称】 青山 葆

【選任した代理人】

    【識別番号】 100086405

    【弁理士】

    【氏名又は名称】 河宮 治

【選任した代理人】

【識別番号】 100113170

【弁理士】

【氏名又は名称】 稲葉 和久

【手数料の表示】

【予納台帳番号】 013262

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証の選択システム、認証システム

【特許請求の範囲】

【請求項 1】 被認証者を認証する少なくとも一つの認証手段を用いた認証に要求される目標性能を満たす、一の認証又は認証の組み合わせを選択する認証手段選択部を備えることを特徴とする認証の選択システム。

【請求項 2】 被認証者を認証する少なくとも一つの認証手段を用いた一の認証又は認証の組合せを生成する組合せ生成部と、

前記一の認証又は認証の組合せごとの認証性能を演算する複合認証性能演算部と

をさらに備えることを特徴とする請求項 1 に記載の認証の選択システム。

【請求項 3】 前記目標性能を設定する目標性能設定部と、

選択する認証の制約条件を設定する制約条件設定部と

をさらに備え、

前記組合せ生成部は、前記制約条件に基づいて一の認証又は認証の組合せを生成し、

前記認証手段選択部は、前記目標性能を満たす一の認証又は認証の組合せの中から、前記制約条件に基づいて一の認証又は認証の組合せを選択することを特徴とする請求項 1 又は 2 に記載の認証の選択システム。

【請求項 4】 前記制約条件は、認証手段の種類、認証手段の種類の優先順位、認証の組合せ方法、認証の組合せ方法の優先順位、組合せる認証の数、組み合わせる認証の数の優先順位、組合せの候補数、のうち少なくとも一つであることを特徴とする請求項 3 に記載の認証の選択システム。

【請求項 5】 前記認証手段の認証性能を記憶しておく性能記憶部と、

前記認証手段による認証結果のログデータを解析し、前記認証手段の認証性能に反映させるログ解析部と

をさらに備えたことを特徴とする請求項 1 から 4 のいずれか一項に記載の認証の選択システム。

【請求項 6】 前記性能記憶部は、登録者ごとの認証性能を記憶しているこ

とを特徴とする請求項 5 に記載の認証の選択システム。

【請求項 7】 前記認証手段の認証性能は、被認証者が登録者本人である場合の入力データと登録データとの一致の度合いを示す照合度の確率密度関数、数値テーブル、確率分布、正規分布で近似した場合のパラメータ、のうち少なくとも一つからなることを特徴とする請求項 1 から 6 のいずれか一項に記載の認証の選択システム。

【請求項 8】 請求項 1 から 7 のいずれか一項に記載の一の認証又は認証の組み合わせを選択する前記認証の選択システムと、

被認証者の入力データを登録データと照合し、被認証者を認証する少なくとも一つの認証手段と、

を備え、

前記認証の選択システムで選択された前記一の認証又は認証の組み合わせによって、前記被認証者を認証することを特徴とする認証システム。

【請求項 9】 被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと  
を含むことを特徴とする認証の組み合わせの選択方法。

【請求項 10】 被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと、

前記選択した一の認証又は認証の組合せによって、被認証者の入力データを登録データと照合して、被認証者を認証するステップと  
を含むことを特徴とする認証方法。

【請求項 1 1】 被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと  
を含むことを特徴とするコンピュータで実行される認証の選択プログラム。

【請求項 1 2】 請求項 1 1 に記載の前記認証の選択プログラムを格納したことを特徴とするコンピュータ読取可能な記録媒体。

【請求項 1 3】 被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと、

前記選択した一の認証又は認証の組合せによって、被認証者の入力データを登録データと照合して、被認証者を認証するステップと  
を含むことを特徴とするコンピュータで実行される認証プログラム。

【請求項 1 4】 請求項 1 3 に記載の前記認証プログラムを格納したことを特徴とするコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、認証手段を用いて被認証者を認証する認証システムに関する。

【0 0 0 2】

【従来の技術】

重要な機密事項に関して、接触できる人を制限して機密保持を行ったり、特定の部屋への入室者のチェックを行う方法には様々な方法がある。例えば、ICカードや、ID、パスワード等の入力によって認証を行う方法がある。しかし、I

CカードやID、パスワード等は登録者本人以外の他人であっても使用することができるため、より厳密なセキュリティが求められる場合には充分ではない。

【0003】

一方、他人に使用されることのない各個人に固有の指紋を用いた認証装置が知られている（特開2000-76450号公報）。この認証装置は、入力された指紋の種類と順番の組合せとを照合している。

【0004】

【発明が解決しようとする課題】

上記認証装置による認証方法は、指紋による認証の機密性を高くするために指紋の入力回数を複数回にし、その入力順序が正しいか否かについても判断している。しかし、この方法では認証の機密性を高めることはできるが、ただ単に指紋の入力回数を複数回にしているだけであって、その結果どのくらいの認証精度が得られるか分からなかった。つまり、要求される認証精度があった時に、指紋の入力を何回にすれば必要な認証精度を確保できるか分からなかった。

【0005】

そこで、本発明の目的は、認証に必要な目標性能を満たす認証手段を用いて被認証者が登録者であるか否か認証する認証システムを提供することである。

【0006】

【課題を解決するための手段】

本発明に係る認証の選択システムは、被認証者を認証する少なくとも一つの認証手段を用いた認証に要求される目標性能を満たす、一の認証又は認証の組み合わせを選択する認証手段選択部を備えることを特徴とする。

【0007】

また、本発明に係る認証の選択システムは、前記認証の選択システムであって、被認証者を認証する少なくとも一つの認証手段を用いた一の認証又は認証の組み合わせを生成する組み合わせ生成部と、

前記一の認証又は認証の組合せごとの認証性能を演算する複合認証性能演算部と  
をさらに備えることを特徴とする。

【 0 0 0 8 】

さらに、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記目標性能を設定する目標性能設定部と、

選択する認証の制約条件を設定する制約条件設定部とをさらに備え、

前記組合せ生成部は、前記制約条件に基づいて一の認証又は認証の組合せを生成し、

前記認証手段選択部は、前記目標性能を満たす一の認証又は認証の組合せの中から、前記制約条件に基づいて一の認証又は認証の組合せを選択することを特徴とする。

【 0 0 0 9 】

またさらに、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記制約条件は、認証手段の種類、認証手段の種類の優先順位、認証の組合せ方法、認証の組合せ方法の優先順位、組合せる認証の数、組み合わせる認証の数の優先順位、組合せの候補数、のうち少なくとも一つであることを特徴とする。

【 0 0 1 0 】

また、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記認証手段の認証性能を記憶しておく性能記憶部と、

前記認証手段による認証結果のログデータを解析し、前記認証手段の認証性能に反映させるログ解析部と

をさらに備えたことを特徴とする。

【 0 0 1 1 】

さらに、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記性能記憶部は、登録者ごとの認証性能を記憶していることを特徴とする。

【 0 0 1 2 】

またさらに、本発明に係る認証の選択システムは、前記認証の選択システムであって、前記認証手段の認証性能は、被認証者が登録者本人である場合の入力デ



ータと登録データとの一致の度合いを示す照合度の確率密度関数、数値テーブル、確率分布、正規分布で近似した場合のパラメータ、のうち少なくとも一つからなることを特徴とする。

【 0 0 1 3 】

本発明に係る認証システムは、一の認証又は認証の組み合わせを選択する前記認証の選択システムと、

被認証者の入力データを登録データと照合し、被認証者を認証する少なくとも一つの認証手段と、  
を備え、

前記認証の選択システムで選択された前記一の認証又は認証の組み合わせによって、前記被認証者を認証することを特徴とする。

【 0 0 1 4 】

本発明に係る認証の選択方法は、被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと  
を含むことを特徴とする。

【 0 0 1 5 】

本発明に係る認証方法は、被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと、

前記選択した一の認証又は認証の組合せによって、被認証者の入力データを登録データと照合して、被認証者を認証するステップと  
を含むことを特徴とする。

【0 0 1 6】

本発明に係るコンピュータで実行される認証の選択プログラムは、被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップとを含むことを特徴とする。

【0 0 1 7】

本発明に係る認証の選択プログラムを格納したコンピュータ読取可能な記録媒体は、前記認証の選択プログラムを格納したことを特徴とする。

【0 0 1 8】

本発明に係るコンピュータで実行される認証プログラムは、被認証者を認証する認証手段を用いた一の認証又は認証の組合せを生成するステップと、

前記一の認証又は認証の組み合わせごとの認証性能を演算し、記憶するステップと、

前記一の認証又は認証の組み合わせの中から、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択するステップと、

前記選択した一の認証又は認証の組合せによって、被認証者の入力データを登録データと照合して、被認証者を認証するステップとを含むことを特徴とする。

【0 0 1 9】

本発明に係る認証プログラムを格納したコンピュータ読取可能な記録媒体は、前記認証プログラムを格納したことを特徴とする。

【0 0 2 0】

【発明の実施の形態】

本発明の実施の形態に係る認証の選択システムと、認証システムについて、添付の図面を参照して以下に説明する。

【0 0 2 1】

## 実施の形態 1.

本発明の実施の形態 1 に係る認証の選択システム及び認証システムについて説明する。この認証の選択システムは、図 1 のブロック図に示すように、コンピュータのメモリ 20 上に読みこまれたプログラムとして、目標性能を設定する目標性能設定部 21 と、選択する認証手段の制約条件を設定する制約条件設定部 22 と、認証手段の認証性能を記憶しておく性能記憶部 23 と、制約条件に基づいて認証手段を用いた認証の組合せを生成する組合せ生成部 24 と、各認証の組合せごとの認証性能を演算する複合認証性能演算部 25 と、制約条件に基づいて認証の組み合わせを選択する認証手段選択部 26 とを備えている。この認証の選択システムでは、認証手段選択部 26 で選択した認証手段を用いた認証の組合せによって被認証者を認証する。これによって目標性能を満たし、しかも制約条件に合う認証手段を用いた認証の組合せによって被認証者を認証することができる。なお、この認証システムは、上記各構成要素に限定されず、他の構成要素を含んでいてもよい。また、メモリ 20 上に読みこまれた上記プログラムは、ハードディスク等の記録媒体上に記録されていてもよい。さらに、上記目標性能設定部 21 と、制約条件設定部 22 と、性能記憶部 23 と、組合せ生成部 24 と、複合認証性能演算部 25 と、認証手段選択部 26 とは、プログラムとしてではなく、ハードウェア的に実現してもよい。なお、この認証の選択システムの構成要素ではないが、被認証者を認証する認証手段としての認証手段 1 (指紋) 11 及び認証手段 2 (虹彩) 12 を用いている。また、上記ソフトウェアの機能実現のためのハードウェアとして、CPU 13、記録媒体に格納されたプログラムを読み取る記録媒体ドライブ 14、入力装置 15、出力装置 16、メモリ 20 等を備えていてもよい。

## 【0022】

ここで、上記認証手段 11、12 について説明する。この認証手段 11、12 によって被認証者を認証する。この「認証」としては、例えば、被認証者の入力データと登録データとを照合して、被認証者が登録者本人であるか否かを判断する認証手続である。なお、これ以外の認証手続を行うものであってもよい。また、認証手段としては、指紋、顔、声、虹彩、掌形、署名などの生体情報と呼ばれ

る各被認証者がもつ身体的特徴あるいは動作によって認証する認証手段の他、パスワードやＩＣカード等の生体とは無関係な認証手段も用いることができる。好ましくは、指紋、顔、声、虹彩等の生体情報を用いて認証する認証手段である。生体情報を用いた認証の場合には、パスワードやＩＣカードの盗用のような他人による登録者への「なりすまし」を防止することができる。なお、「認証手段を用いた一の認証又は認証の組合せ」とは、少なくとも一つの認証手段を用いた少なくとも一つの認証を含んでいればよく、また、複数の認証手段を用いた認証の組合せに限られない。また、同一の認証手段を用いた認証を複数回組み合わせてもよい。さらに、各認証の組合せは、AND、OR、NOT等の論理演算による場合の他、線形和や重み付き線形和等を用いてもよい。

#### 【0023】

次に、認証手段の認証性能について説明する。指紋や虹彩等の生体情報による認証を行う認証手段では、通常、登録データと入力データとの一致の度合を示す照合度という値が求められ、その照合度がある一定の閾値を越えるか否かで被認証者が本人であるかどうかを判断する。認証手段の認証性能は、例えば、被認証者が登録者本人であるのに、該登録者本人ではない他人と認証される誤認証（F R : false rejection）の割合であるF R R（false rejection rate）と、被認証者が該登録者本人ではない他人（以下、「他人」という）であるのに、該登録者本人と認証される誤認証（F A : false acceptance）の割合であるF A R（false acceptance rate）とによって表わされる。なお、複数の登録者がある場合には、被認証者はある登録者本人ではあるが、別の登録者本人と誤って認証される誤認証（F A）がある。このF R RやF A Rは、設定する閾値によって変化するため、図4の（a）に示すように、閾値による関数として表わされる。また、F R RとF A Rとは、図4の（a）に示すように、トレードオフの関係にあり、一方を上げれば、もう一方は下がる性質がある。さらに、図4の（b）は、被認証者が登録者本人である場合の本人照合度と、被認証者が該登録者本人でない他人である場合の他人照合度について、それぞれ照合度に対する頻度を示すグラフである。図4の（a）のF R R及びF A Rを閾値（照合度）で微分したものが図4の（b）の本人照合度分布及び他人照合度分布に相当する。したがって、逆に

、図 4 の ( b ) の本人照合度分布及び他人照合度分布を照合度について積分すると、図 4 の ( a ) の F R R、F A R にそれぞれ相当する。そこで、認証手段の認証性能として、図 4 の ( a ) 又は ( b ) のいずれのデータで記憶してもよい。なお、これ以外の方法で認証性能を定めてもよい。

#### 【 0 0 2 4 】

認証システムが稼動を始める初期状態の場合など、蓄積されている実際の照合データが少ない場合には、単一の認証手段の認証性能は、使用する認証手段のセンサベンダが提供する認証性能特性を用いる。しかし、以下の手順で実際の照合データを用いて、単一の認証手段の性能を求めることが望ましい。各々の単一の認証手段の認証性能の算出は、実際の認証に先だってあらかじめ、図 3 のフローチャートに示すように、次の手順で行われる。

( 1 ) あらかじめ、システム管理者によって入力装置 1 5 から入力された登録者の登録データを C P U 1 3 で受け取って、ハードディスク等の記録媒体等に登録しておく。

( 2 ) 次に、各認証手段 1 1、1 2 から被認証者の照合データを C P U 1 3 で受け取る ( 1 1 1 )。なお、次の手順は、照合データのうち、被認証者が登録者本人同士の照合データと、被認証者が互いに他人同士である照合データとに分けて行う。

( 3 - 1 ) まず、被認証者が登録者本人である場合の照合データの処理手順を示す。この場合に、照合データのうち、同一の登録者本人の各照合ごとの照合データ間での照合を C P U 1 3で行って、本人照合度を算出する ( 1 1 2 )。

( 4 - 1 ) 本人照合度の頻度分布を C P U 1 3 で確率密度関数化する ( 1 1 3 )。なお、ここでは照合度分布の表現方法として確率密度関数を用いたが、これに限られず、例えば、確率分布や正規分布等の標準的な分布関数で近似した場合の平均や分散等のパラメータを用いて表現してもよい。

( 3 - 2 ) 次に、被認証者が互いに他人同士である場合の照合データの処理手順を示す。この場合に、照合データのうち、他人同士の照合データ間での照合を C P U 1 3で行って、他人照合度を算出する ( 1 1 4 )。

( 4 - 2 ) 他人照合度の頻度分布を C P U 1 3 で確率密度関数化する ( 1 1 5 )

。なお、この場合にも、上述のように照合度分布の表現方法は確率密度関数に限られず、例えば、確率分布や正規分布等の標準的な分布関数で近似した場合の平均や分散等のパラメータを用いて表現してもよい。

(5) 本人照合度分布と他人照合度分布をそれぞれ性能記憶部 2 3 に記憶する (1 1 6)。

以上の手順によって、例えば、図 4 の (b) に示す本人照合度分布と、他人照合度分布を得ることができる。

#### 【 0 0 2 5 】

また、図 4 の (b) に示す本人照合度分布において、設定した閾値と F R R との関係について、図 5 の (a) を用いて説明する。被認証者の照合度  $x_1$  に対して、図 5 の (a) に示すように、閾値  $T_1$  を設定すると、照合度  $x_1$  が閾値  $T_1$  より低い斜線部では、被認証者が登録者本人であるのに該登録者本人ではない他人と認証されてしまう誤認証 (F R) がある。この斜線部が本人照合度分布の全体に占める割合が F R R である。同様に、図 4 の (b) に示す他人照合度分布において、設定した閾値と F A R との関係について、図 5 の (b) を用いて説明する。被認証者の照合度  $x_1$  に対して、図 5 の (b) に示すように、閾値  $T_1'$  を設定すると、照合度  $x_1$  が閾値  $T_1'$  より高い斜線部は、被認証者が登録者本人ではない他人であるのに該登録者本人と認証されてしまう誤認証 (F A) がある。また、複数の登録者がある場合、被認証者はある登録者本人ではあるが、別の登録者本人であると誤って認証される誤認証 (F A) がある。この斜線部が他人照合度分布の全体に占める割合が F A R である。なお、ここでは、斜線部を明確に示す説明の便宜上、閾値  $T_1$  と  $T_1'$  とはそれぞれ異なる値として示したが、実際には同一の閾値について、それぞれの F R R と F A R とを算出する。

#### 【 0 0 2 6 】

この認証システムにおける認証動作は、図 2 のフローチャートに示す以下の手順で行われる。なお、ハードウェアの利用に関して、一般的なコンピュータを構成する CPU、メモリ、記録媒体ドライブ、記録媒体等を用いることができる。

(1) あらかじめ、システム管理者は、被認証者が登録者本人ではない他人であるのに、該登録者本人であると誤って認証する割合 (F A R) 等の目標性能を目

標性能設定部 2 1 で設定しておき、選択する認証の組合せに関する条件としての制約条件を制約条件設定部 2 2 で設定しておく。この場合、ハードウェアの利用に関して、コンピュータの CPU 1 3 ではシステム管理者によって入力装置 1 5 を介して入力された目標性能と制約条件を受け取り、それぞれハードディスク等の記録媒体に記録しておく。

(2) 次に、制約条件設定部 2 2 で設定された制約条件に基づいて、認証手段を用いた一の認証又は認証の組合せを組合せ生成部 2 4 で生成する (1 0 1)。この場合、ハードウェアの利用に関して、CPU 1 3 は記録媒体に記録された制約条件を読み込んで、一の認証又は認証の組合せを生成し、ハードディスク等の記録媒体に記録しておく。この時、生成される一の認証又は認証の組合せを図 9 の (a) の左列に示した。

(3) さらに、各認証の組み合わせごとの認証性能を複合認証性能演算部 2 5 で演算し、各組合せごとに認証性能を性能記憶部 2 3 に記憶する (1 0 3)。この場合、ハードウェアの利用に関して、CPU 1 3 で各認証の組合せごとの認証性能を演算し、記録媒体に記録している。

(4) そして、全ての認証と、全ての認証の組合せについて認証性能の演算を行ったか否かを CPU 1 3 で判断する (1 0 3)。なお、全ての組合せについて演算していなければ、再度手順 1 0 2 を実行する。

(5) 全ての認証と全ての認証の組合せについて演算を行い、記憶させた場合には、目標性能を満たす全ての認証と認証の組合せの中から認証手段選択部 2 6 で制約条件に基づいて一の認証又は認証の組み合わせを選択する (1 0 4)。なお、ハードウェアの利用に関して、CPU 1 3 で一の認証又は認証の組合せを選択する。

以上の手順によって、目標性能を満たす一の認証又は認証の組み合わせを選択することができる。また、選択した一の認証又は認証の組合せによって、目標性能を確保して被認証者の認証を行うことができる。なお、目標性能の設定は、例えば、指紋や顔などのバイオメトリクスによる本人認証を部屋の入退室時に行う場合であれば、認証の対象とする複数の部屋のそれぞれについて設定しておいてもよい。この場合に、被認証者が入室を希望する部屋を選択した際に、認証手段

の選択を行う。

【0027】

次に、上記フローチャートの各手順について説明する。まず、目標性能設定部 21 で目標性能を設定する上記手順について説明する。目標性能の設定は、精度の高い認証を必要とする場合、例えば非常に重要な施設への入退室のドアの開閉についての認証には高い目標性能を設定し、一方、中程度の精度の認証を必要とするコンピュータへのログインの場合にはそれに見合った目標性能を目標性能設定部 21 で設定すればよい。先にあげた例を用いれば、非常に重要な施設への入退室は、登録者本人が登録者でないと認証される割合の FRR が高くとも、他人が誤って登録者と認証される割合の FAR を低く抑えたい。この場合、目標性能としては (FRR, FAR) = (3.0%, 0.001%) 等のようにシステム管理者が設定する。一方、コンピュータのログインでは、それほどセキュリティを重視せず利便性を重視するのであれば、目標性能としては (FRR, FAR) = (0.1%, 0.1%) 等のようにシステム側によって設定する。

【0028】

また、制約条件設定部 22 で選択する認証の組合せに関する制約条件を設定する上記手順について説明する。ここで制約条件とは、認証の組合せの選択にあたって、用いる認証手段の種類やその優先順位、複数の認証手段を用いた認証を組合せる最大数、さらに、認証を組合せる方法やその優先順位等の条件である。例えば、重要施設のドアであれば、制約条件として、認証手段の候補を指紋と虹彩とし、最大の組合せ数を 4、組合せ方法を AND と設定することができる。また、コンピュータログインであれば、制約条件として認証手段の候補は指紋と顔と声とし、最大の組合せ数は 3、組合せ方法は AND、OR、重み付き線形和等と設定することができる。

【0029】

さらに、図 2 の各組み合わせの複合認証性能を演算し、記憶する手順 102 について、図 6 のフローチャートを用いて説明する。

(1) まず、認証手段を用いた認証の組合せについて、CPU 13 で複合認証モデルを作成する (121)。なお、この手順 121 については後述する。



(2) 次に、各認証手段の認証性能を性能記憶部 2 3 から読み込む (1 2 2)。ハードウェアの利用に関しては、各認証手段の認証性能を記録媒体から読みこむ。

(3) 各認証手段の照合度  $x_1$ 、 $x_2$  の閾値  $T_1$ 、 $T_2$  の初期値を設定する (1 2 3)。例えば、照合度の範囲が 0 から 1 0 0 と設定している場合には、初期値  $(T_1, T_2) = (0, 0)$  と設定してもよい。

(4) 設定した閾値  $T_1$ 、 $T_2$  による認証性能 (FRR、FAR) を算出する (1 2 4)。ハードウェアの利用としては、CPU 1 3 で上記認証性能を算出する。

(5) 設定した閾値  $T_1$ 、 $T_2$  の複合認証性能を記憶する (1 2 5)。ハードウェアの利用としては、記録媒体に記録する。

(6) 閾値  $T_1$ 、 $T_2$  の設定を全範囲で行ったか否かを CPU 1 3 で判断する (1 2 6)。閾値の設定が全範囲で行われていなかった場合には閾値を更新し (1 2 8)、手順 1 2 4 に戻って複合認証性能を算出する。この閾値の更新は、例えば、いずれか一方の閾値を 1 ずつ増していてもよい。また、その刻み幅は、各認証手段で得られる照合度の精度に応じて設定すればよい。例えば、照合度の制度が小数点以下一桁であれば、0. 1 刻みに、小数点二桁の精度があれば 0. 0 1 刻みで変化させればよい。

(7) 閾値の設定を全範囲で行った後、目標性能を満たす閾値の範囲を CPU 1 3 で探索する (1 2 7)。この手順については後述する。

以上の手順によって、目標性能を満たす各組合せの認証性能を演算し、記憶させることができる。

#### 【0 0 3 0】

ここで、制約条件として、例えば、認証手段の種類に関して指紋を優先し、認証手段を用いた認証の組合せ数が少ない組合せを優先するという条件がある場合には、認証手段選択部によって、図 9 の (a) に示す関係の中から条件に合わせて優先度の高い順番に並べ替え、最終的な認証の組み合わせとして、図 9 の (b) のような組合せを選択する。これによって、目標性能を満たす認証の組合せの中から上記制約条件を満たす認証の組合せを選択することができる。なお、図 9

では、簡略化するために、各認証の組合せについて指紋の照合度の閾値（T1）と虹彩の照合度の閾値（T2）とを一組しか示していない。しかし、実際には、目標性能を満たすための閾値の組合せ（T1，T2）は、これ以外にも所定の範囲にわたって取り得る場合がある。また、一定の刻み幅で設定する場合、その組合せは多数存在し、これらを用いることができる。

## 【0031】

次に、上記図6の手順について、認証手段を用いた認証の組合せが「指紋と虹彩の重み付き線形和」の例によって説明する。

（1）まず、各認証手段の認証性能を読み込む。この例では、認証手段としての指紋による本人照合度の確率密度関数  $f_1(x_1)$  と、他人照合度分布の確率密度関数  $g_1(x_1)$  および虹彩の本人照合度の確率密度関数  $f_2(x_2)$ 、他人照合度分布の確率密度関数  $g_2(x_2)$  を性能記憶部23から読み出す。ハードウェアの利用としては、記録媒体から読み出す。ここで、添え字の1および2は、それぞれ認証手段としての指紋および虹彩を意味しており、 $x_1$ 、 $x_2$  は、それぞれ認証手段として指紋および虹彩による照合度を意味する。

（2）この認証の組合せ「指紋と虹彩の重み付き線形和」について、複合認証性能モデルを作成する。まず、下記式に示す重み付き線形和に対応した新しい変数  $z$  を設定する。

## 【数1】

$$z = \text{weightsum}(x_1 - T_1, x_2 - T_2) = w_1(x_1 - T_1) + w_2(x_2 - T_2) \quad (1)$$

## 【0032】

この変数  $z$  は、この認証の組合せにおいて、0または正の値をとる場合には被認証者は登録者本人であると判断し、負の値をとる場合には被認証者は他人であると判断する変数である。また、変数  $z$  を構成する  $\text{weightsum}()$  関数は、各引数にそれぞれ重み係数をかけて線形和の演算を行う関数であり、 $w_1$  および  $w_2$  はそれぞれ指紋の照合度  $x_1$  および虹彩の照合度  $x_2$  に対する重み係数である。この  $w_1$ 、 $w_2$  は、それぞれの認証手段に対する認証の依存度を表わしたパラメータである。

## 【0033】

次に、被認証者が登録者本人である場合の変数  $z$  の確率密度関数を  $F(z, T_1, T_2)$  と表記し、被認証者が他人である場合の  $z$  の確率密度関数を  $G(z, T_1, T_2)$  と表記する。それぞれの認証手段による認証結果が互いに独立である場合には、式 (1) の  $z$  についての確率密度関数は、それぞれの確率密度関数の積で表わすことができるので、それぞれ下記式 (2) 及び式 (3) で表わすことができる。

【数 2】

$$F(z, T_1, T_2) = \int_{-\infty}^{+\infty} f_1(x'_1) f_2(x'_2) dx'_1 = \int_{-\infty}^{+\infty} f_1(x'_1) f_2((z - w_1 \cdot x'_1) / w_2) dx'_1 \quad (2)$$

【数 3】

$$G(z, T_1, T_2) = \int_{-\infty}^{+\infty} g_1(x'_1) g_2(x'_2) dx'_1 = \int_{-\infty}^{+\infty} g_1(x'_1) g_2((z - w_1 \cdot x'_1) / w_2) dx'_1 \quad (3)$$

なお、式 (2) および式 (3) では、 $x'_1 = x_1 - T_1$ 、 $x'_2 = x_2 - T_2$  という変数変換を行って、それぞれ  $x'_1$ 、 $x'_2$  の関数として表わしている。また、ここでは各認証手段による認証結果について互いに独立であると想定したが、それぞれの認証結果の間に一定の相関関係を有する場合には、相関係数等を考慮して構成することができる。

【0 0 3 4】

上記式 (1) のように設定した変数  $z$  において、 $z$  が 0 もしくは正の時、登録者本人と判断し、 $z$  が負の場合に他人と判断するものとする。これにより、図 6 の上記手順 1 2 4 において、被認証者が登録者本人であるのに、該登録者本人でないと判断される割合  $FRR$  と、被認証者が他人であるのに登録者本人であると判断される割合  $FAR$  とは、 $F(z, T_1, T_2)$  および  $G(z, T_1, T_2)$  を用いて下記式 (4) 及び式 (5) で表わされる。

【数 4】

$$FRR(T_1, T_2) = \int_{-\infty}^0 F(z, T_1, T_2) dz \quad (4)$$

【数 5】

$$FAR(T1, T2) = \int_0^{\infty} G(z, T1, T2) dz \quad (5)$$

【0035】

上記式（４）及び式（５）によって以上のように複合認証の方法に従って変数  $z$  を設定すれば、登録者本人の  $z$  の確率密度関数  $F(z, T1, T2)$  および他人の  $z$  の確率密度関数  $G(z, T1, T2)$  が決定でき、 $F(z, T1, T2)$  が負となる条件から  $FRR$  の、 $G(z, T1, T2)$  が正となる条件から  $FAR$  の複合認証性能モデルを作成することができる。

【0036】

また、「指紋と虹彩との  $AND$  認証」を考える。この場合には、 $AND$  演算であるので、認証手段として指紋によって登録者本人と認証し、かつ、虹彩によって登録者本人と認証された場合にのみ被認証者は登録者本人と認証される。この場合に、被認証者が登録者本人であるか否かを判断する上記変数は、下記式（６）で表わされる。すなわち、 $AND$  認証の場合は、上記重み付き線形和認証の場合の式（１）を式（６）に置き換えることで複合認証性能モデルを作成することができる。

【数 6】

$$z = \min(x1 - T1, x2 - T2) \quad (6)$$

【0037】

ここで、 $\min()$  は引数の最小値を求める関数である。上記と同様に、式（６）で表わされる変数  $z$  が 0 又は正の値をとる場合には登録者本人と判断し、負の場合には他人と判断する。したがって、被認証者が登録者本人であるのに、該登録者本人でないと誤って認証される場合（ $FR$ ）は、指紋と虹彩とによる照合度  $x1$ 、 $x2$  の少なくとも一方がそれぞれの閾値  $T1$ 、 $T2$  を越えなかった場合に発生する。一方、被認証者が他人の場合に該登録者本人と誤って認証される場合（ $FA$ ）は、指紋と虹彩との照合度  $x1$ 、 $x2$  の両方がそれぞれの閾値  $T1$ 、 $T2$  を越えた場合に発生する。なお、登録者が複数ある場合には、被認証者があ

## 【0038】

さらに、「指紋と虹彩とのOR認証」を考える。この場合には、OR演算であるので、認証手段として指紋によって登録者本人と認証するか、または、虹彩によって登録者本人と認証された場合に被認証者は登録者本人と認証される。この場合に、被認証者が登録者本人であるか否かを判断する上記変数は、下記式(7)で表わされる。すなわち、OR認証の場合は、上記重み付き線形和認証の場合の式(1)を式(7)に置き換えることで複合認証性能モデルを作成することができる。

## 【数7】

$$z = \max(x1 - T1, x2 - T2) \quad (7)$$

## 【0039】

ここで、 $\max()$  は引数の最大値を求める関数である。上記と同様に、式(7)で表わされる変数  $z$  が0又は正の値をとる場合には登録者本人と判断し、負の場合には他人と判断する。したがって、被認証者が登録者本人であるのに、該登録者本人でないと誤って認証される場合(FR)は、指紋と虹彩とによる照合度  $x1$ 、 $x2$  の両方がそれぞれの閾値  $T1$ 、 $T2$  を越えなかった場合に発生する。一方、被認証者が他人の場合に該登録者本人と誤って認証される場合(FA)は、指紋と虹彩との照合度  $x1$ 、 $x2$  の少なくとも一方がそれぞれの閾値  $T1$ 、 $T2$  を越えた場合に発生する。なお、登録者が複数ある場合には、被認証者がある登録者本人であるが、別の登録者本人と誤って認証される場合(FA)がある。また、他の論理演算等や、これ以外の複合認証方法においても、式(1)に示す変数  $z$  の定義を変更することによって、その複合認証性能モデルを作成することができる。

## 【0040】

次に、図6の上記手順127について、図7のフローチャートを用いて説明する。

(1) まず、閾値の初期値を設定する(131)。この閾値の初期値の設定は、上記図6の手順123と同様に行うことができる。

(2) 設定した閾値に対応する複合認証性能 (FRR, FAR) を記録媒体から読み込む (132)。

(3) 読みこんだ認証性能が目標性能 (FRR, FAR) を満たすか否かを判断する (133)。例えば、指紋と虹彩の組み合わせにおいて、目標性能として (FRR, FAR) = (3.0%, 0.001%) と設定されている場合、設定された閾値 T1、T2 に対応して読みこまれた認証性能 (FRR, FAR) を上記目標性能のそれぞれの値と比較することによって目標性能を満たすか否かの判断を CPU13 で行う。

(4) 手順 133 で設定した閾値による認証性能の値が目標性能を満たしていると判断された場合、その場合の閾値を記録媒体に記憶させる (134)。一方、手順 133 で設定した閾値による認証性能の値が目標性能を満たしていないと CPU13 で判断された場合には、この手順 134 を飛ばして次の手順 135 に移る。

(5) 次いで、閾値の設定を全範囲で行ったか CPU13 で判断する (135)。閾値の設定を全範囲で済ませていた場合には終了する。

(6) 一方、手順 135 で閾値の設定が済んでいない範囲があれば閾値の更新をして (136)、手順 132 に戻る。

#### 【0041】

さらに、図 2 の目標性能を満たす認証の組合せの中から、制約条件に基づいて認証の組合せを選択する手順 104 について、図 8 及び図 9 の (a)、(b) を用いて説明する。

(1) 制約条件に基づいて生成された各認証の組み合わせについて、目標性能を満たす閾値を記録媒体から読みこむ (141)。例えば、図 9 の (a) に示す表のように、認証の組合せと目標性能を満たす閾値との組合せである。

(2) 目標性能を満たす閾値があるか否かを CPU13 で判断する (142)。

(3) 手順 142 で目標性能を満たす閾値がある場合には、その認証の組合せの種類と閾値とを記録媒体に記憶する (143)。一方、手順 142 で目標性能を満たす閾値がない場合には、手順 143 を迂回する。

(4) 全ての組合せを読みこんだか否かを CPU13 で判断する (144)。読

みこんでいない組合せがあれば、対象の組合せを次の組合せに更新して（１４７）、手順１４１へ移る。

（５）一方、手順１４４で全ての組合せについて読みこんだとＣＰＵ１３で判断した場合には、目標性能を満たす閾値が存在する組合せを制約条件の優先順位に基づいて配列する（１４５）。例えば、制約条件として、認証手段に指紋を用いた場合の優先順位が高い場合には、図９の（ａ）に挙げられている組合せのうち、図９の（ｂ）に示すように配列される。

（６）配列の先頭にある認証の組合せをＣＰＵ１３で選択する（１４６）。なお、この認証の組合せの選択に関しては、単一の制約条件によって配列する場合に限られず、複数の制約条件によって配列し、選択してもよい。

#### 【００４２】

なお、この認証の選択システムでは、認証手段として指紋と虹彩の例を挙げたが、他の認証手段であっても、 $f_1()$ 、 $f_2()$ が他の認証手段の確率密度関数に置き換わるだけであり、同様の複合認証性能モデルを適用できる。また、認証を組み合わせる数が３以上の場合にも、それぞれの確率密度関数が $f_1()$ 、 $f_2()$ 、 $f_3()$ と順次増えるだけであり、同様のモデルを適用できる。

#### 【００４３】

さらに、この実施の形態１では、認証手段として指紋、虹彩等の例をあげたが、これに限られず種々の認証手段を用いることができる。また、認証手段を用いた認証の組合せ最大数として４の例をあげたが、これに限られず所望の数を設定してもよい。さらに、認証の組合せ方法として重み付き線形和、AND演算、それにOR演算の例をあげたが、これに限られず、種々の演算方法を用いてもよい。

#### 【００４４】

また、この認証の選択システムをコンピュータ上で実行する認証の選択プログラムは、図２に示すように、下記手順からなる。

（１）あらかじめ、システム管理者によって入力装置１５から入力された登録者本人を登録者でないと誤って認証する割合（FRR）等の目標性能をコンピュータで受け取り、記録媒体に記録しておき、システム管理者によって入力装置１５

から入力された選択する認証の組合せに関する条件としての制約条件を受け取り、記録媒体に記録しておく。

(2) 次に、設定した制約条件に基づいて、CPU 13 等で認証の組合せを生成する (101)。

(3) さらに、各組み合わせごとの認証性能を CPU 13 で演算し、各組合せごとの認証性能を記録媒体等に記憶する (103)。

(4) そして、すべての組合せについて認証性能の演算を行ったか否かを CPU 13 で判断する (103)。なお、全ての組合せについて演算していなければ、再度手順 102 を実行する。

(5) 全ての組合せについて演算を行い、記憶させた場合には、上記認証の組合せの中から制約条件に基づいて認証の組み合わせを CPU 13 で選択する (104)。

以上の手順によって、この認証の選択システムをコンピュータ上で実行し、目標性能を満たす認証の組合せを選択し、目標性能を確保して被認証者の認証を行うことができる。

#### 【0045】

さらに、上記認証の選択プログラムをコンピュータで読み取ることができる記録媒体に格納してもよい。このようにコンピュータ読取可能な記録媒体に格納することによって可搬性を備え、この認証の選択システムを稼働させることが容易に行うことができる。また、この認証の選択プログラムは、電子通信回線を通じて搬送することができるので、さらに遠隔地においても容易に実行させることができる。

#### 【0046】

なお、上記コンピュータ読取可能な記録媒体としては、フレキシブルディスク、ハードディスク、等の磁気記録媒体、CD-ROM、CD-R、CD-RW、DVD等の光記録媒体、MO、MD等の光磁気記録媒体、EEPROM、DRAM、フラッシュメモリ等の半導体記録媒体を用いることができる。また、これらの記録媒体に格納された認証の選択プログラムは記録媒体読取装置で読み取られ、コンピュータ上で実行される。



## 【 0 0 4 7 】

次に、この認証システムについて説明する。この認証システムは、図 1 のブロック図に示すように、上記認証の選択システムと、被認証者を認証する認証手段としての認証手段 1（指紋） 1 1 及び認証手段 2（虹彩） 1 2 とを備えている。また、この認証システムは、さらに CPU 1 3、記録媒体に格納されたプログラムを読み取る記録媒体ドライブ 1 4、入力装置 1 5、出力装置 1 6、メモリ 2 0 等を備えている。なお、この認証システムは、上記各構成要素に限定されず、他の構成要素を含んでいてもよい。この認証システムの構成要素である認証の選択システムは、上述の通り、メモリ 2 0 上に読みこまれたプログラムとして、ハードウェアである CPU 1 3 等によってその機能を実現している。この認証システムでは、認証の選択システムによって選択された認証手段を用いた一の認証又は認証の組合せによって、各認証手段 1 1、1 2 を用いて被認証者を認証する。これによって目標性能を満たし、しかも制約条件に合う認証手段を用いた認証の組合せによって被認証者を認証することができる。

## 【 0 0 4 8 】

次に、この認証システムにおける認証方法について、図 1 1 のフローチャートを用いて説明する。この認証システムの認証方法は、実施の形態 1 に係る認証の選択方法の手順を含んでいる。そのため、この認証方法は、図 2 に示す認証の選択方法の手順 1 0 4 まで同一である。さらに、この手順 1 0 4 の後、手順 1 0 5 では、選択した認証手段を用いた一の認証又は認証の組み合わせを用いて、被認証者を認証している（1 0 5）。

## 【 0 0 4 9 】

また、この認証方法をコンピュータ上で実行する認証プログラムは、図 1 1 に示すように、下記手順からなる。

（1）あらかじめ、システム管理者によって入力装置 1 5 から入力された登録者本人を登録者でないと誤って認証する割合（FRR）等の目標性能をコンピュータで受け取り、記録媒体に記録しておき、システム管理者によって入力装置 1 5 から入力された選択する認証の組合せに関する条件としての制約条件を受け取り、記録媒体に記録しておく。

(2) 次に、設定した制約条件に基づいて、CPU 1 3 等で認証の組合せを生成する (1 0 1)。

(3) さらに、各組み合わせごとの認証性能を CPU 1 3 で演算し、各組合せごとの認証性能を記録媒体等に記憶する (1 0 3)。

(4) そして、すべての組合せについて認証性能の演算を行ったか否かを CPU 1 3 で判断する (1 0 3)。なお、全ての組合せについて演算していなければ、再度手順 1 0 2 を実行する。

(5) 全ての組合せについて演算を行い、記憶させた場合には、上記認証の組合せの中から制約条件に基づいて認証の組み合わせを CPU 1 3 で選択する (1 0 4)。

(6) 選択した認証の組合せによって被認証者の認証を行う (1 0 5)。

以上の手順によって、この認証システムをコンピュータ上で実行し、目標性能を満たす認証を選択し、目標性能を確保して被認証者の認証を行うことができる。

#### 【 0 0 5 0 】

さらに、上記認証プログラムをコンピュータで読み取ることができる記録媒体に格納してもよい。このようにコンピュータ読取可能な記録媒体に格納することによって可搬性を備え、この認証システムを稼働させることが容易に行うことができる。また、この認証プログラムは、電子通信回線を通じて搬送することができるので、さらに遠隔地においても容易に実行させることができる。

#### 【 0 0 5 1 】

なお、上記コンピュータ読取可能な記録媒体としては、フレキシブルディスク、ハードディスク、等の磁気記録媒体、CD-ROM、CD-R、CD-RW、DVD等の光記録媒体、MO、MD等の光磁気記録媒体、EEPROM、DRAM、フラッシュメモリ等の半導体記録媒体を用いることができる。また、これらの記録媒体に格納された認証プログラムは記録媒体読取装置で読み取られ、コンピュータ上で実行される。

#### 【 0 0 5 2 】

実施の形態 2.

本発明の実施の形態 2 に係る認証の選択システム及び認証システムについて説明する。まず、この認証の選択システムについて説明する。この認証の選択システムは、実施の形態 1 に係る認証の選択システムと比較すると、図 1 1 のメモリ 2 0 に示すように、実際に認証を行っていく中で蓄積するログデータを解析するログ解析部 2 7 を備えている点で相違する。このログ解析部 2 7 によって実際の認証結果に対応して、それぞれの認証手段の認証性能に動的に反映させることができる。なお、ログ解析部 2 8 は CPU 1 3 上で実行されるプログラムによって実現される。

## 【 0 0 5 3 】

この認証の選択システムは、あらかじめ性能記憶部 2 3 に記憶されている各認証手段 1 1、1 2 の認証性能 (FRR、FAR) について、実際の認証で得られるログデータを解析し、各認証手段の認証性能を更新している。例えば、ある認証で認証手段として指紋が用いられた場合、このログデータとして照合時の入力データを残しておく。ログ解析部 2 8 は、残された照合時の入力データを用いて、被認証者が登録者本人と認証された場合と、被認証者が他人と認証された場合とに分類する。次いで、登録者本人同士のデータ相互の照合による本人照合度分布と、他人同士のデータ相互の照合による他人照合度分布とを算出することができる。このように認証が行われるごとに各認証手段による実際の認証実績が記憶されていくため、その結果を統計処理し、既存の各認証手段の認証性能を更新することができる。このように実際の認証実績を各認証手段の認証性能に反映させることによって、より実際の認証の実性能に基づいて認証を選択できる。

## 【 0 0 5 4 】

このログデータを解析し、各認証手段による認証性能へ反映する手順の詳細について、図 1 2 及び図 1 3 のフローチャートを用いて以下に説明する。まず、被認証者が登録者本人と認証されたログデータを本人照合度分布に反映させる場合について、図 1 2 を用いて以下に説明する。

(1) ログデータの中で、登録者本人と認証された照合データ、照合度を記録媒体からそれぞれ順に読み込む (1 5 1)。

(2) 照合度は所定のデータ反映用閾値以上であるか否かを CPU 1 3 で判断す

る（152）。

（3）上記手順152で照合度が所定の反映用閾値以上の場合には、その照合データを登録者本人データとして記録媒体に記憶する（153）。上記手順152で照合度が所定値より低い場合には反映用としては用いないこととする。この場合に、本人と判定する閾値よりも高いデータ反映用閾値を設定し、照合度が上記のデータ反映用閾値を越えたデータのみを反映用のデータとして用いるのが好ましい。これによってデータ反映の信頼度を高めることができる。

（4）次に、対象となるログデータを全て読み込んだか否かをCPU13で判断する（154）。読みこんでいないログデータがあれば手順151に戻って読みこむ。

（5）登録者ごとに登録者本人とされた各照合データ間についてCPU13によって相互に照合を行って、本人照合度を算出する（155）。

（6）ログデータによる本人照合度の頻度分布を算出する（156）。

（7）全登録者に関する既存の本人照合度分布にログデータによる本人照合度分布を反映させ、本人照合度分布を更新する（157）。ハードウェアの利用としては、記録媒体から読みこんだ本人照合度分布に上記ログデータによる本人照合度分布を追加し、更新する。これによって、本人照合度の確率密度関数の積分であるFRRにも反映させることができる。

#### 【0055】

また、被認証者が登録者本人と認証されたログデータを他人照合度分布に反映させる場合について、図13を用いて以下に説明する。

（1）ログデータの中で、登録者本人と認証された照合データ、照合度を記録媒体からそれぞれ順に読み込む（161）。

（2）照合度が所定のデータ反映用閾値以上であるか否かをCPU13で判断する（162）。

（3）上記手順162で照合度が所定の反映用閾値以上の場合には、その照合データを登録者本人データとして記録媒体に記憶する（163）。上記手順162で照合度が所定値より低い場合には反映用としては用いないこととする。この場合に、登録者本人と判定する閾値よりも高いデータ反映用閾値を設定し、照合度

が上記のデータ反映用閾値以上のデータのみを反映用のデータとして用いるのが好ましい。これによってデータ反映の信頼度を高めることができる。

(4) 次に、対象となるログデータを全て読み込んだか否かをCPU13で判断する(164)。読みこんでいないログデータがあれば手順161に戻って読みこむ。

(5) 登録者本人とされた照合データについて、互いに異なる他人の照合データ間についてCPU13で相互に照合を行って、他人照合度を算出する(165)。

(6) ログデータによる他人照合度の頻度分布を算出する(166)。

(7) 全登録者に関する既存の他人照合度分布にログデータによる他人照合度分布を反映させ、他人照合度分布を更新する(167)。ハードウェアの利用に関しては、記録媒体から読みこんだ他人照合度分布に上記ログデータによる他人照合度分布を追加して更新している。これによって、他人照合度の確率密度関数の積分であるFARにも反映させることができる。

#### 【0056】

なお、このログ解析による反映は、ログが増えるごとに行ってもよく、あるいは所定数のログが蓄積された場合に行ってもよい。また、所定時間ごと、例えば、1日1回行ってもよい。さらに、ログからの照合データ抽出は、前回の処理以降に記録されたログについて行えばよい。また、相互に照合するデータとしては、新たなログのデータのみで行ってもよく、あるいは古いデータを含めて相互に照合してもよい。

#### 【0057】

次に、この認証システムについて説明する。この認証システムは、実施の形態1に係る認証システムと比較すると、図11に示すように、上記認証の選択システムに関する相違と同様に、メモリ20内にログ解析部27を備えている点で相違する。また、上記認証の選択システムをコンピュータ上で実行するためのハードウェアとして、実施の形態1に係る認証システムと同様に、認証手段11、12を備えるとともに、CPU13、記録媒体ドライブ14、入力装置15、出力装置16を備えている。

## 【 0 0 5 8 】

## 実施の形態 3.

本発明の実施の形態 3 に係る認証の選択システムについて説明する。この認証の選択システムは、各々の認証手段の認証性能を全登録者でのデータとしてのみ有している実施の形態 1 及び 2 に係る認証の選択システムと比較すると、各々の認証手段の認証性能を各登録者ごとのデータとして保存している点で相違する。これによって、登録者を ID 等で特定して被認証者の認証を行う場合には、各登録者ごとにより最適な認証の組合せ、閾値等の認証条件を選択することができる。

## 【 0 0 5 9 】

また、上記実施の形態 2 に係る認証の選択システムに示す場合と同様に、実際の認証のログデータを解析して、その結果を各認証手段の認証性能に反映させることができる。この場合には、各登録者ごとの本人照合度および F R R、他人照合度および F A R を算出し、既存の各登録者ごとの本人照合度分布および F R R、他人照合度分布および F A R を更新する。これによって実際の認証結果に基づいた本人照合度分布、他人照合度分布を用いて特定登録者ごとの最適な認証を選択することができる。なお、特定の登録者についての他人照合度分布とは、その登録者本人のデータとその登録者以外の他人との間の相互に照合された照合度を意味している。また、この場合には、あらかじめ認証の対象となる登録者が特定されていることが前提となる。

## 【 0 0 6 0 】

なお、このログ解析による反映は、ログが増えるごとに行ってもよく、あるいは所定数のログが蓄積された場合に行ってもよい。また、所定時間ごと、例えば、1 日 1 回行ってもよい。さらに、ログからの照合データ抽出は、前回の処理以降に記録されたログについて行えばよい。また、相互に照合するデータとしては、新たなログのデータのみで行ってもよく、あるいは古いデータを含めて相互に照合してもよい。

## 【 0 0 6 1 】

## 実施の形態 4.

本発明の実施の形態 4 に係る認証の選択システムについて説明する。この認証の選択システムは、実施の形態 1 に係る認証の選択システムと比較すると、図 1 4 に示すように、制約条件として認証手段の種別の優先順位を設定する点で相違する。上記実施の形態 1 で示したように、目標性能を満たす一の認証又は認証の組合せは複数存在する場合がある。この認証の選択システムでは、制約条件設定部 2 2 で認証手段の種別の優先順位を設定している。これによって適切な一の認証又は認証の組合せを選択することができる。なお、この制約条件としては、認証手段の種類、その優先順位、組合せる最大数、組み合わせる数の優先順位、認証の組合せ方法、組合せ方法の優先順位、認証の組合せの候補数、などを設定することができる。また、認証手段の種類別の優先順位として、認証手段の各種類の特性、例えば、処理時間、処理コスト、使用エネルギー等によってそれぞれことなる優先順位を決めてもよい。この場合、処理時間の速さに基づく認証手段の種類別の優先順位としては、例えば、指紋が最も処理時間が速く、2 番目に顔、3 番目に虹彩である。

#### 【 0 0 6 2 】

次に、図 1 4 に示す認証手段の種類別の優先順位によって、各組み合わせを配列する場合の手順を以下に示す。

(1) まず、認証の組合せの候補が複数ある場合には、制約条件である図 1 4 の認証手段の優先順位に基づいて、認証手段選択部 2 6 において一の認証及び認証の組合せを並べ替える。この並べ替えでは、図 1 4 の認証手段の優先順位として、指紋の優先順位が最も高いので、まず認証手段に指紋を含む一の認証又は認証の組合せを選ぶ。次に、優先順位が 2 番目の虹彩を含む一の認証又は認証の組合せを選ぶ。図 9 の (a) に示す一の認証又は認証の組合せと目標性能を満たす閾値との関係があれば、図 1 5 の表に示すように並び替えられる。

(2) 次に、最も優先順位が高い一の認証又は認証の組合せが最終候補として CPU 1 3 によって選択される。

以上のようにして、認証手段の種別の優先順位を与えることによって最終候補を絞りこむことができる。

#### 【 0 0 6 3 】

## 実施の形態 5.

本発明の実施の形態 5 に係る認証の選択システムについて説明する。この認証の選択システムは、実施の形態 4 に係る認証の選択システムと比較すると、制約条件として、認証の組合せ方法（演算方法）の優先順位及び組合せる認証の数の優先順位を設定する点で相違する。この制約条件によって、目標性能を満たす認証の組合せが複数存在する場合であっても適切な認証の組合せを絞り込むことができる。

## 【 0 0 6 4 】

具体的には、この認証の選択システムは、制約条件として、図 1 6 に示すように、認証の組合せ方法の優先順位を設定している。この制約条件は、制約条件設定部 2 2 で設定される。目標性能を満たす認証の組合せの候補が複数存在する場合に、認証手段選択部 2 6 で、図 1 6 に示す認証の組合せ方法の優先順位に基づいて配列する。この図 1 6 の例では重み付き線形和の優先順位が最も高いので、まず認証の組合せ方に重み付き線形和を含む組合せを選び、次に優先順位が 2 番目の AND 演算を含む組合せを選ぶ。以上のようにして、認証の組合せ方法の優先順位を与えることによって最終候補を絞りこむことができる。なお、制約条件として、組み合わせる認証の数を設定してもよい。

## 【 0 0 6 5 】

## 実施の形態 6.

本発明の実施の形態 6 に係る認証の選択システムについて説明する。この認証の選択システムは、実施の形態 1 から 5 に係る認証の選択システムと比較すると、制約条件として、最終的に選択される認証の組合せの候補数を限定している点で相違する。これによって、設定した候補数以内で認証の組合せを選択するので、迅速に認証の組合せを選択できる。

## 【 0 0 6 6 】

## 実施の形態 7.

本発明の実施の形態 7 に係る認証の選択システムについて説明する。この認証の選択システムは、実施の形態 1 に係る認証の選択システムと比較すると、制約条件として認証手段の種類の選択条件を設定する代わりに、あらかじめ使用でき



る認証手段の種類をシステムに接続されている認証手段を識別することによって自動的に行うことができる点で相違する。これによって、選択する認証手段の種類を制約条件として入力しておく必要がなくなり、認証手段の変更を行った場合にも自動的に識別して選択の対象とすることができる。なお、認証手段の識別にあたっては、認証手段である指紋認証装置等进行操作することによってセンサの有無を判定し、自動的に識別させてもよい。

## 【 0 0 6 7 】

実施の形態 8.

本発明の実施の形態 8 に係る認証の選択システムについて説明する。この認証の選択システムは、上記実施の形態 1 から 7 に係る認証の選択システムと比較すると、認証手段選択部で認証手段を用いた認証の組み合わせを選択する場合に、制約条件の適用を段階的に行う点で相違する。これによって、認証の組合せの選択を 1 回で行うのではなく、それぞれ異なる制約条件を別々に適用して総合的に適切な認証の組合せを選択することができる。また、多段階に制約条件を適用することによって認証の組合せを絞り込んで選択してもよい。

## 【 0 0 6 8 】

## 【発明の効果】

本発明に係る認証の選択システムによれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択する認証手段選択部を備えている。これによって、高い認証性能を持つ一の認証又は認証の組合せを適切に選択し、高い精度で認証を行うことができる。

## 【 0 0 6 9 】

また、本発明に係る認証の選択システムによれば、一の認証又は認証の組合せを生成する組合せ生成部と、生成した一の認証又は認証の組合せの認証性能を演算する複合認証性能演算部とを備えている。これによって各々の認証手段の認証性能から複数の認証手段を用いた認証の組合せ等の認証性能を求めることができる。そこで、一の認証や認証の組合せにおける精度向上の程度を推定することができ、必要な認証性能を備えた一の認証又は認証の組合せを選択できる。

## 【 0 0 7 0 】

さらに、本発明に係る認証の選択システムによれば、選択する認証に関する制約条件を設定している。これによって、目標性能を満たす認証の組合せが複数存在する場合にも、制約条件に基づいて一の認証又は認証の組合せを選択することができる。

## 【 0 0 7 1 】

またさらに、本発明に係る認証の選択システムによれば、制約条件として認証手段の種類、認証手段の種類の優先順位等を設定している。これによって、適切な一の認証又は認証の組合せを選択できる。

## 【 0 0 7 2 】

また、本発明に係る認証の選択システムは、実際の認証のログデータを解析して、各認証手段の認証性能に反映させている。これによって実際の認証実績に応じて適切な一の認証又は認証の組合せを選択することができる。

## 【 0 0 7 3 】

またさらに、本発明に係る認証の選択システムは、性能記憶部で登録者ごとの認証性能を記憶させている。これによって、各登録者ごとにより適切な認証の組合せを選択することができる。

## 【 0 0 7 4 】

さらに、本発明に係る認証の選択システムは、認証性能として、被認証者が登録者本人である場合の本人照合度の確率密度関数、数値テーブル、確率分布、正規分布で近似した場合のパラメータ、のうちから選択できる。

## 【 0 0 7 5 】

本発明に係る認証システムは、上記認証の選択システムと、被認証者を認証する少なくとも一つの認証手段とを備えている。これによって、認証の選択システムで選択した最適な認証の組合せにより、各認証手段を用いた精度の高い認証を行うことができる。

## 【 0 0 7 6 】

本発明に係る認証の選択方法によれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択している。これによって、選択した一の認証又は認証の組合せによって、高い精度で被認証者を認証することができる。

【0077】

本発明に係る認証方法によれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択し、選択した一の認証又は認証の組合せによって被認証者を認証している。これによって、高い精度で認証することができる。

【0078】

本発明に係る認証の選択プログラムによれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択している。これによって、選択された一の認証又は認証の組合せによって、高い精度で被認証者を認証することができる。

【0079】

本発明に係る認証の選択プログラムを格納したコンピュータ読取可能な記録媒体によれば、可搬性に優れるので、上記認証の選択システムを容易にコンピュータ上で稼動することができる。

【0080】

本発明に係る認証プログラムによれば、認証に要求される目標性能を満たす一の認証又は認証の組合せを選択し、選択した一の認証又は認証の組合せによって被認証者を認証している。これによって、高い精度で認証することができる。

【0081】

本発明に係る認証プログラムを格納したコンピュータ読取可能な記録媒体によれば、可搬性に優れるので、上記認証システムを容易にコンピュータ上で稼動することができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態1に係る認証の選択システム及び認証システムのブロック図である。

【図2】 本発明の実施の形態1に係る認証の選択のフローチャートである。

【図3】 各認証手段の認証性能を演算するフローチャートである。

【図4】 (a) は認証手段の認証性能であるFRR、FARと閾値との関係を示すグラフであり、(b) は(a)のFRRとFARをそれぞれ微分して得られる本人照合度分布と他人照合度分布を示すグラフである。

【図 5】 (a) は本人照合度分布について、設定した閾値による認証の誤り (F R) との関係を示すグラフであり、(b) は他人照合度分布について、設定した閾値による認証の誤り (F A) との関係を示すグラフである。

【図 6】 図 2 の各組み合わせの複合認証性能を演算し、記憶する手順 1 0 2 の詳細を示すフローチャートである。

【図 7】 図 6 の手順 1 2 7 の詳細を示すフローチャートである。

【図 8】 図 2 の手順 1 0 4 の詳細を示すフローチャートである。

【図 9】 (a) は認証の組合せと目標性能を満たす各認証手段の閾値との関係を示す表であり、(b) は (a) を制約条件に基づいて並べ替えた表である。

【図 1 0】 本発明の実施の形態 1 に係る認証システムによる認証方法のフローチャートである。

【図 1 1】 本発明の実施の形態 2 に係る認証の選択システム及び認証システムのブロック図である。

【図 1 2】 本発明の実施の形態 2 に係る認証の選択システムにおいて、ログデータのうち、登録者本人と認証されたログデータを本人照合度分布へ反映させる手順のフローチャートである。

【図 1 3】 本発明の実施の形態 2 に係る認証の選択システムにおいて、ログデータのうち、登録者本人と認証されたログデータを他人照合度分布へ反映させる手順のフローチャートである。

【図 1 4】 本発明の実施の形態 4 に係る認証の選択システムにおいて、認証手段の種類に優先順位を設けた制約条件の表である。

【図 1 5】 図 1 4 の制約条件に基づいて並べ替えた認証の組合せを示す表である。

【図 1 6】 本発明の実施の形態 5 に係る認証の選択システムにおいて、認証の組合せ方法に優先順位を設けた制約条件の表である。

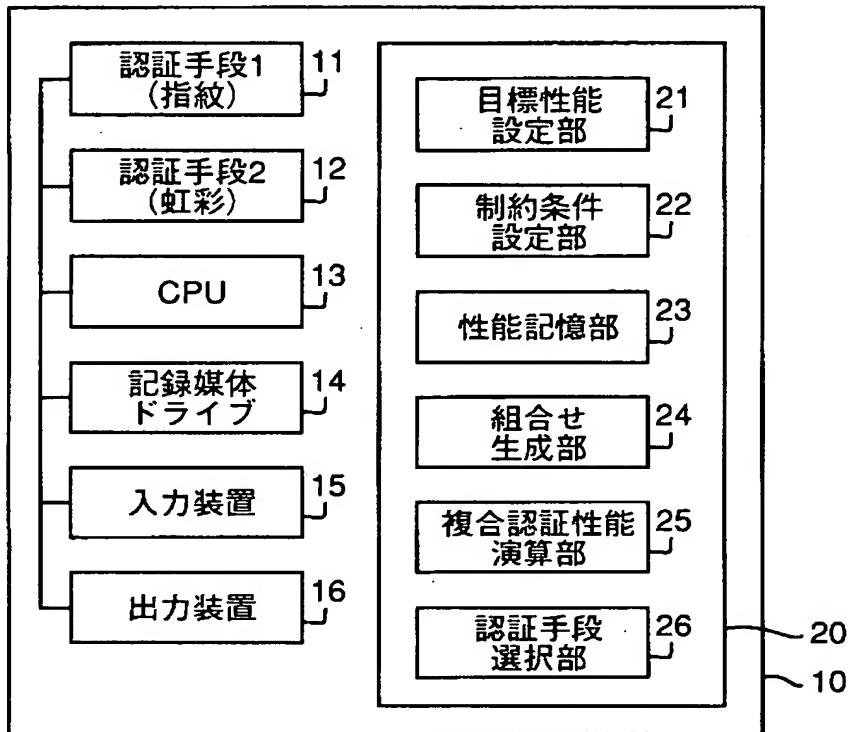
#### 【符号の説明】

1 0 認証システム、1 1 認証手段 1 (指紋)、1 2 認証手段 2 (虹彩)、  
1 3 C P U、1 4 記録媒体ドライブ、1 5 入力装置、1 6 出力装置、2

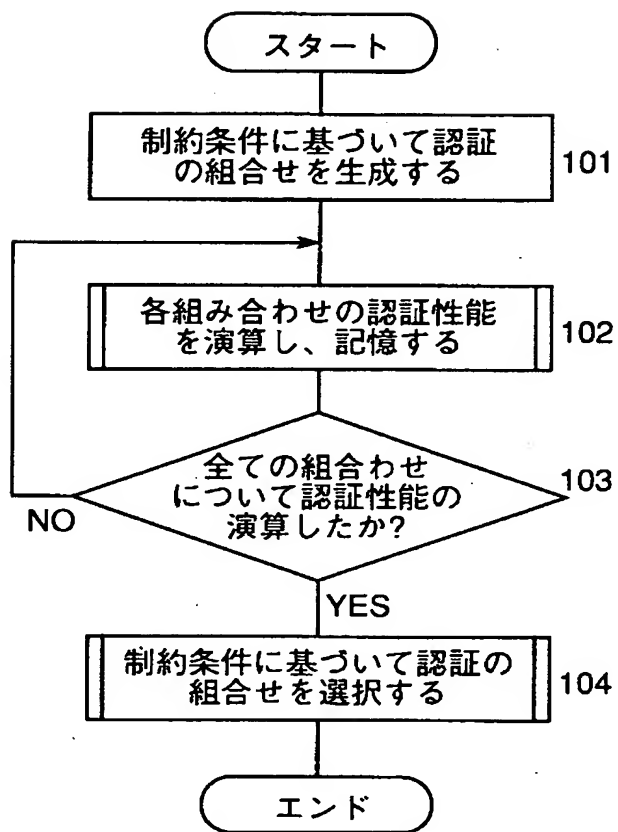
0 メモリ、2 1 目標性能設定部、2 2 制約条件設定部、2 3 性能記憶部  
、2 4 組合せ生成部、2 5 複合認証性能演算部、2 6 認証手段選択部、2  
7 ログ解析部

【書類名】 図面

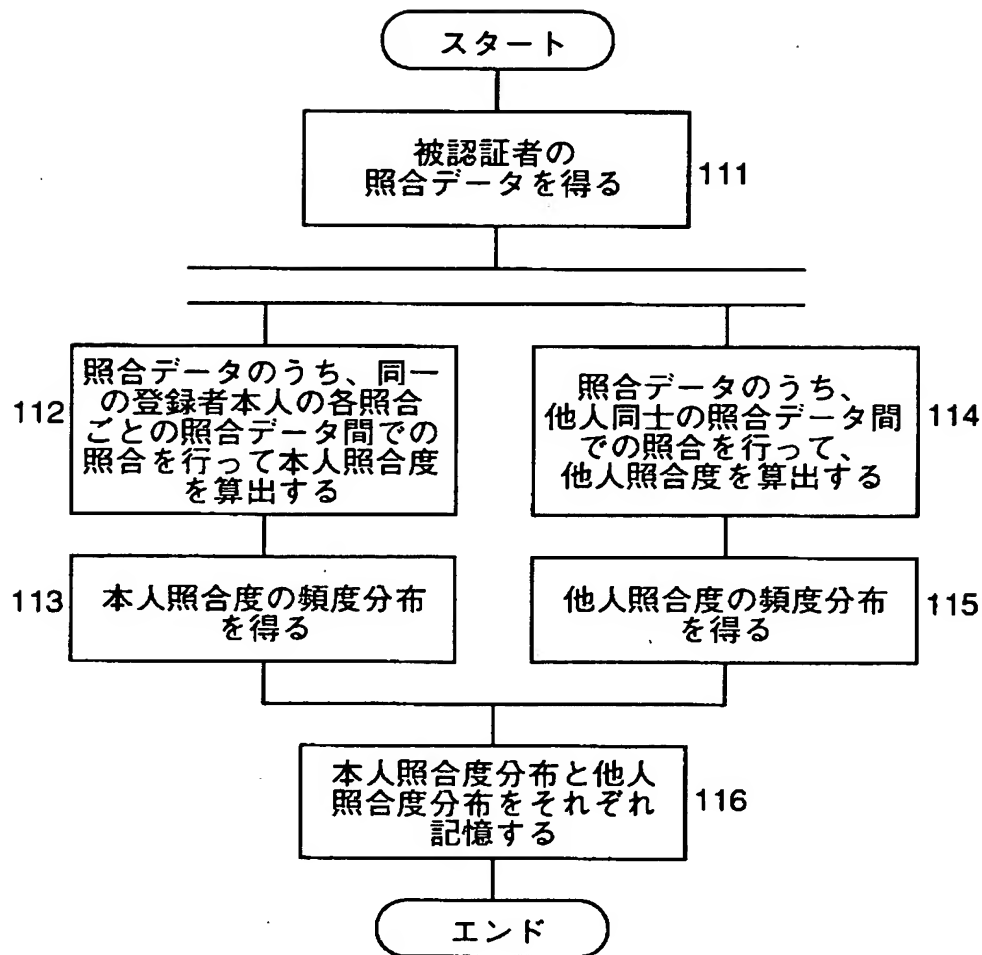
【図1】



【図 2】



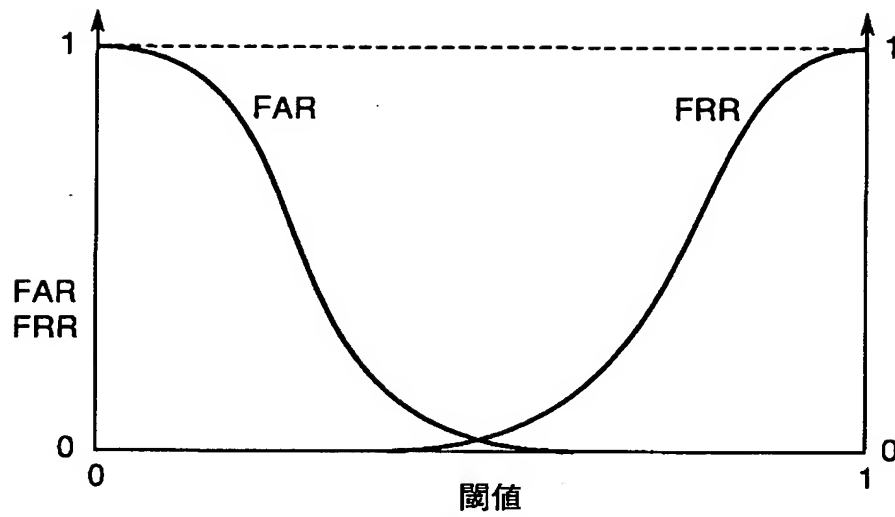
【図 3】



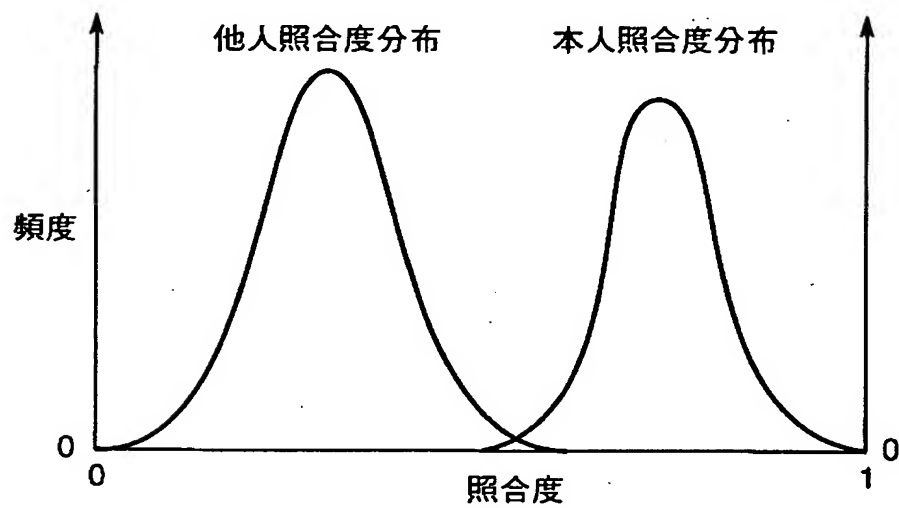


【図4】

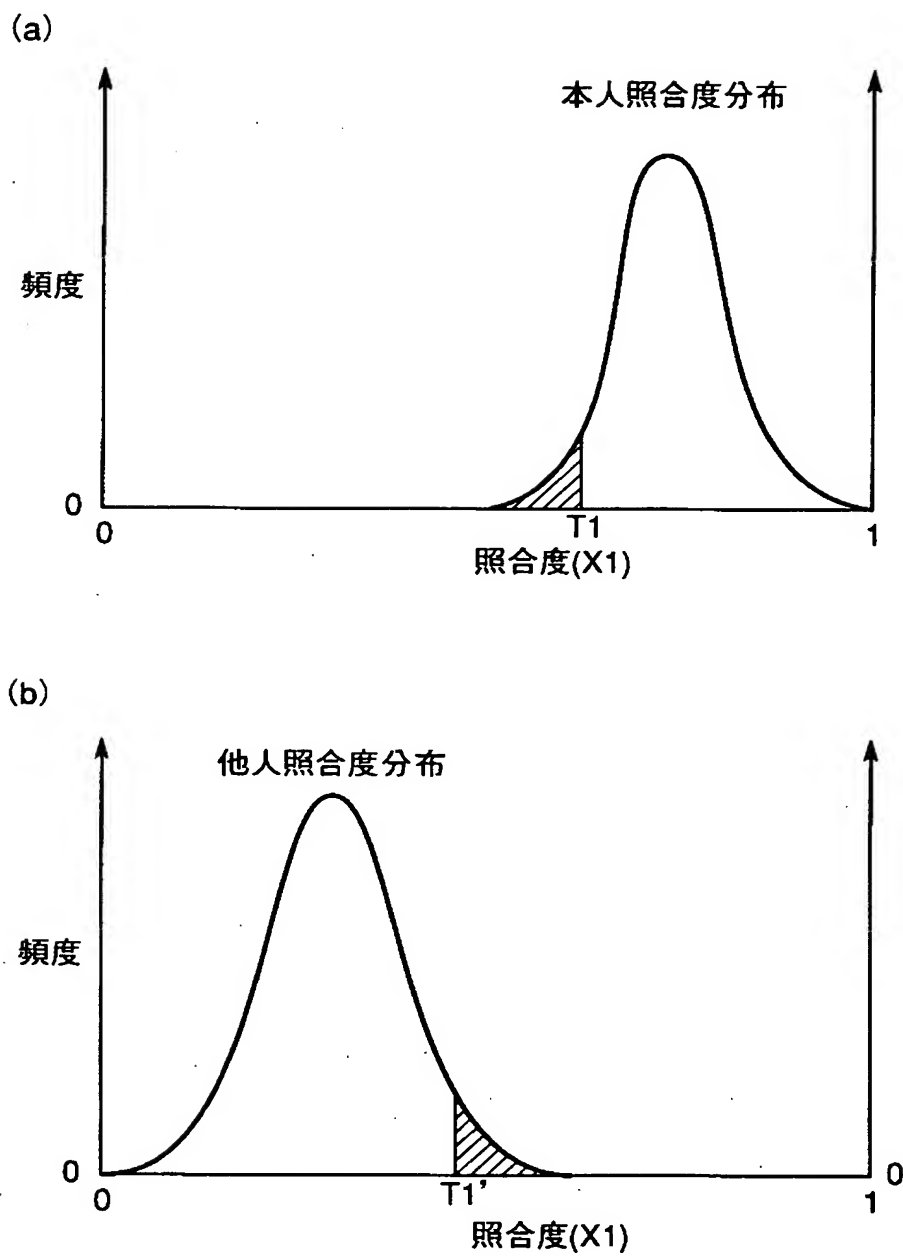
(a)



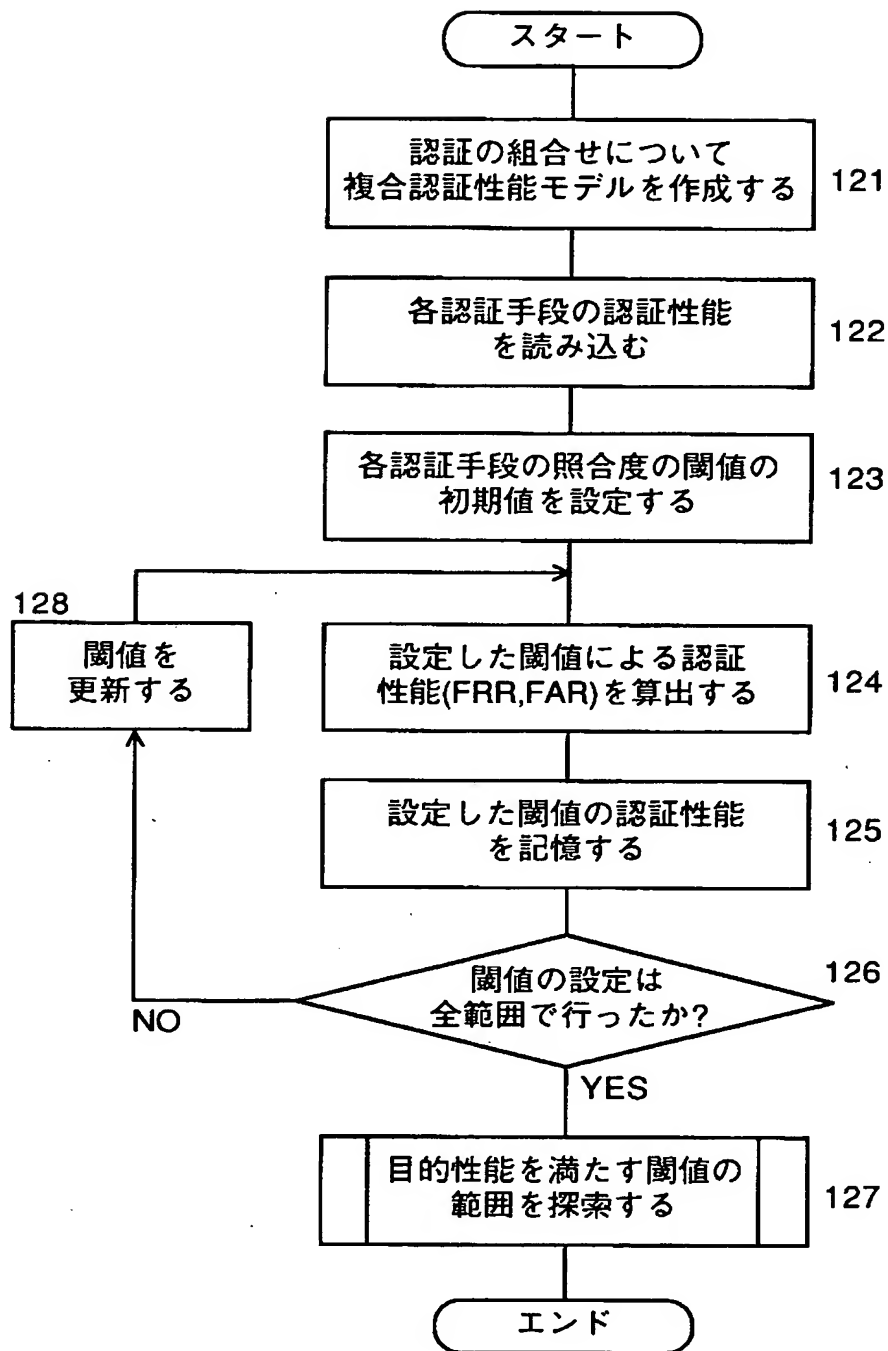
(b)



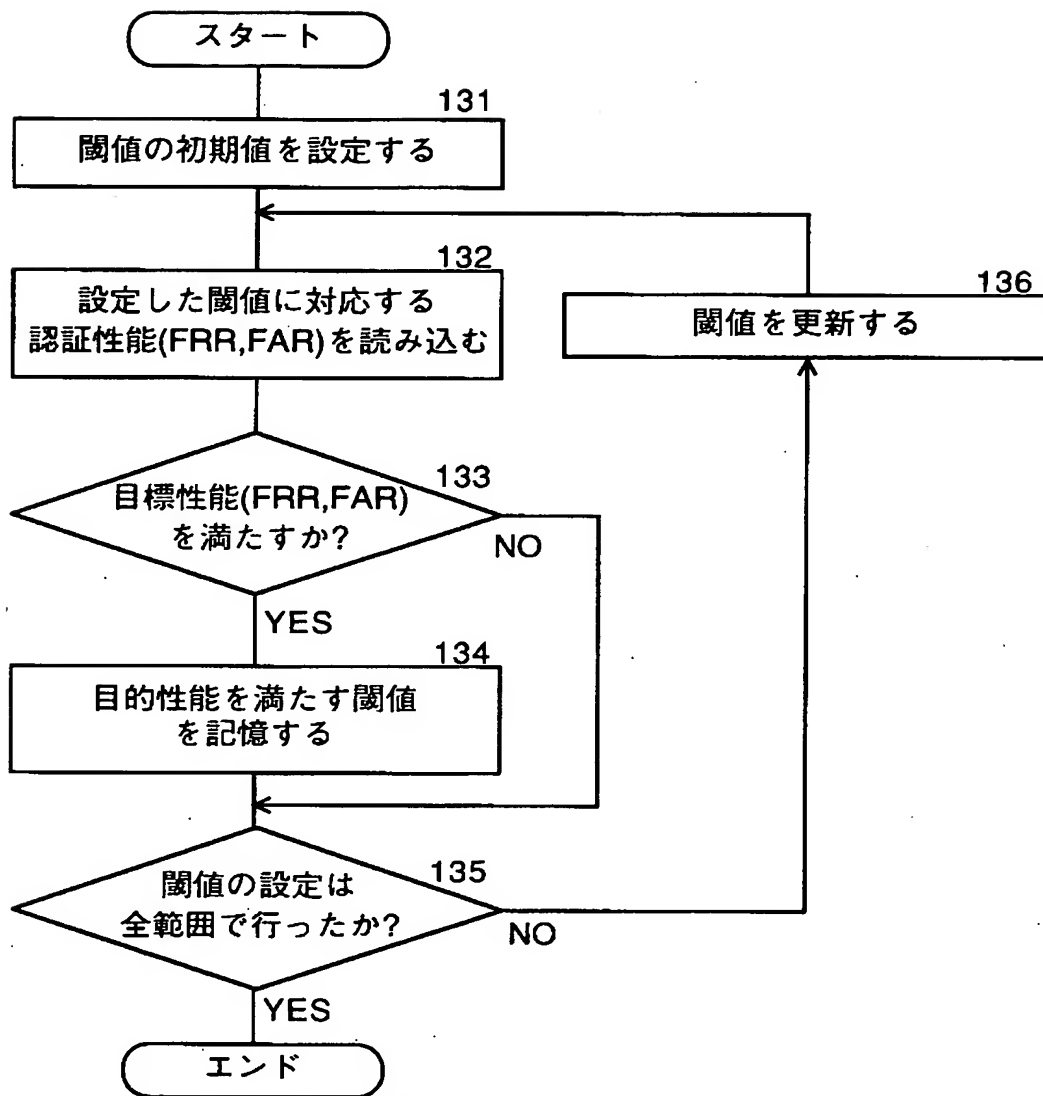
【図 5】



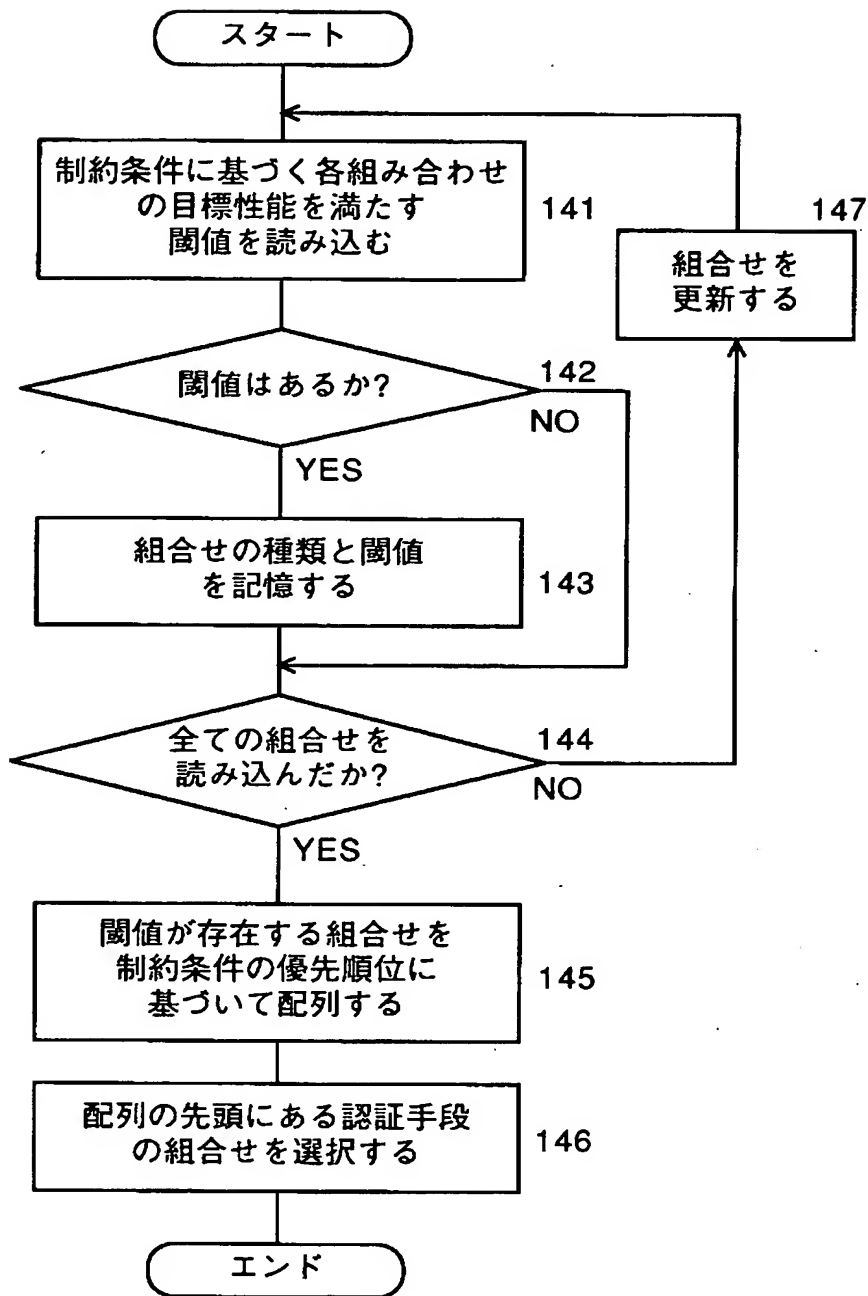
【図 6】



【図 7】



【図 8】



【図9】

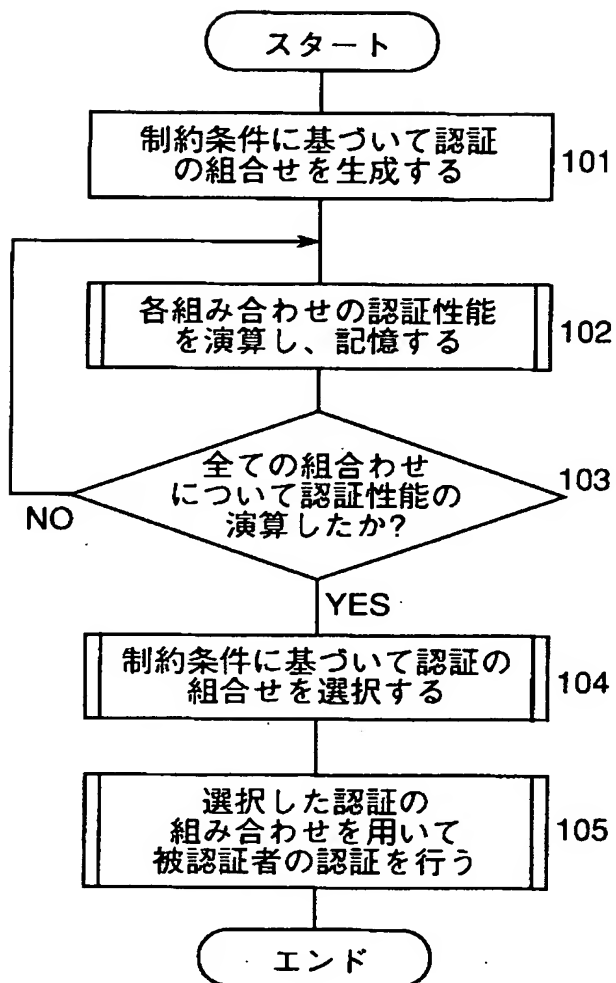
(a)

認証の組合せ	指紋の照合度の閾値 (T1)	虹彩の照合度の閾値 (T2)
指紋AND指紋AND虹彩AND虹彩	35	40
指紋AND虹彩AND虹彩	40	40
指紋AND指紋AND虹彩	35	45
虹彩AND虹彩	—	50
指紋AND虹彩	55	50
指紋AND指紋	60	—
虹彩	—	55
指紋	なし	—
指紋OR虹彩	なし	なし

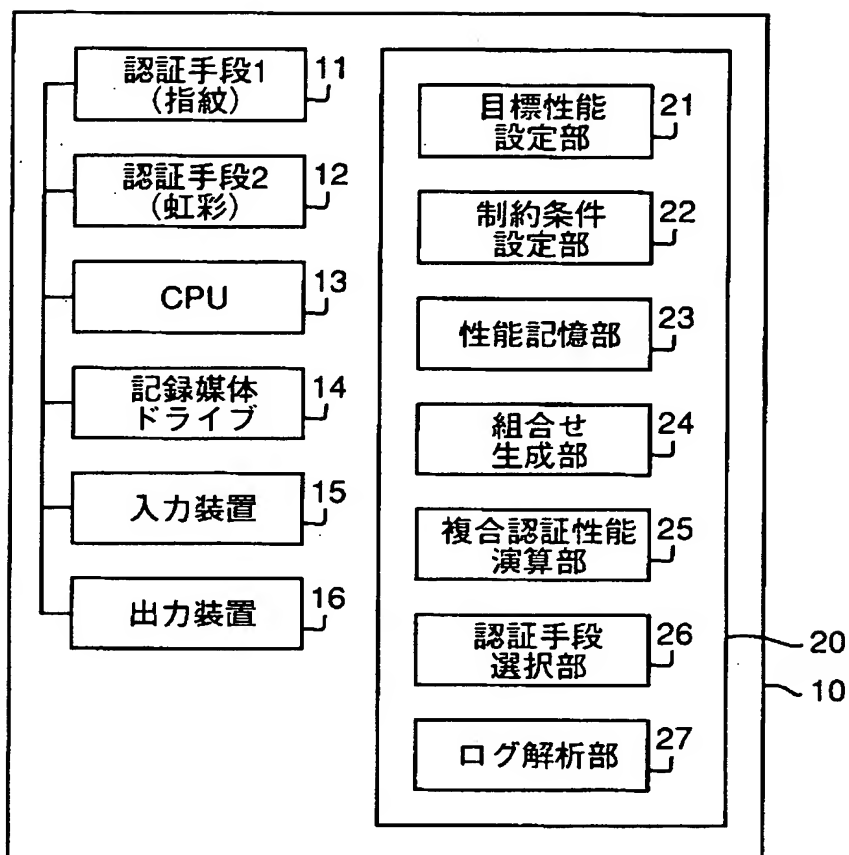
(b)

認証の組合せ	指紋の照合度の閾値 (T1)	虹彩の照合度の閾値 (T2)
指紋AND指紋	60	—
指紋AND虹彩	55	50
指紋AND指紋AND虹彩	35	45
指紋AND虹彩AND虹彩	40	40
指紋AND指紋AND虹彩AND虹彩	35	40
虹彩	—	55
虹彩AND虹彩	—	50

【図10】

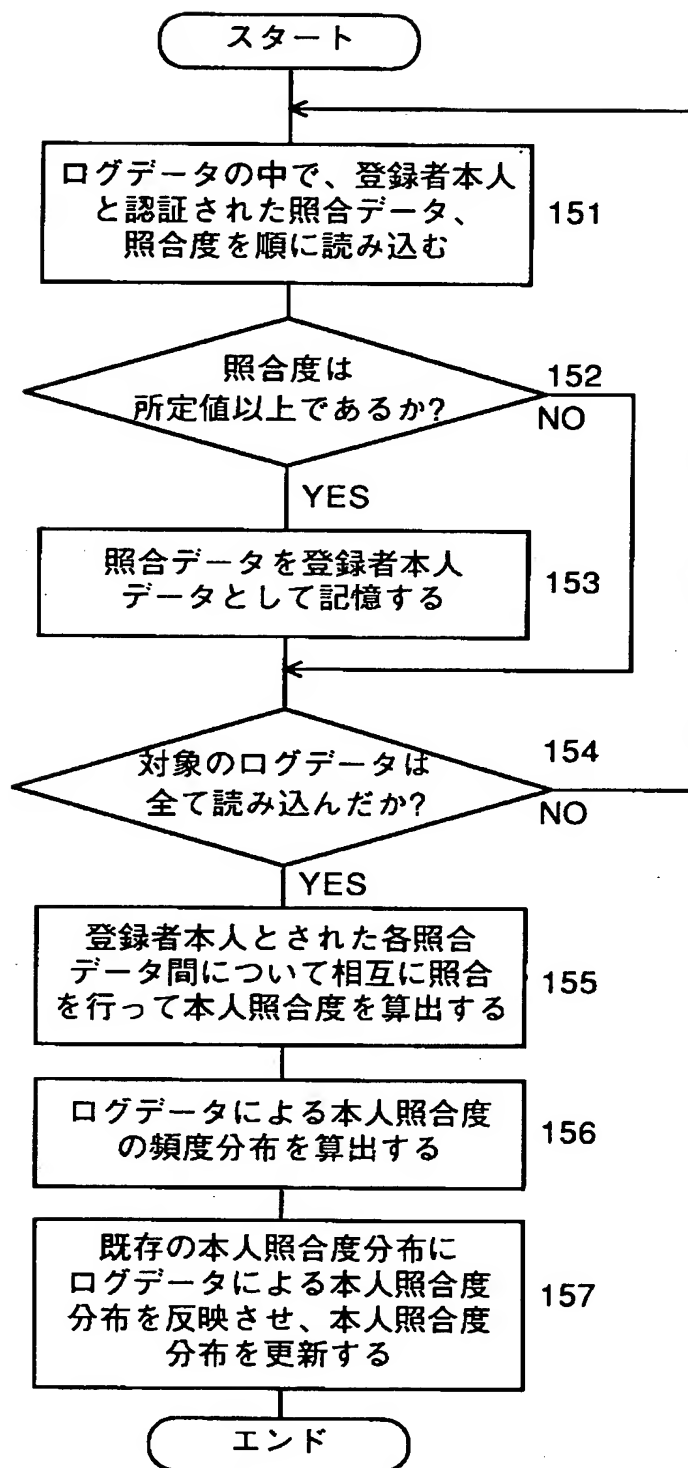


【図 1 1】

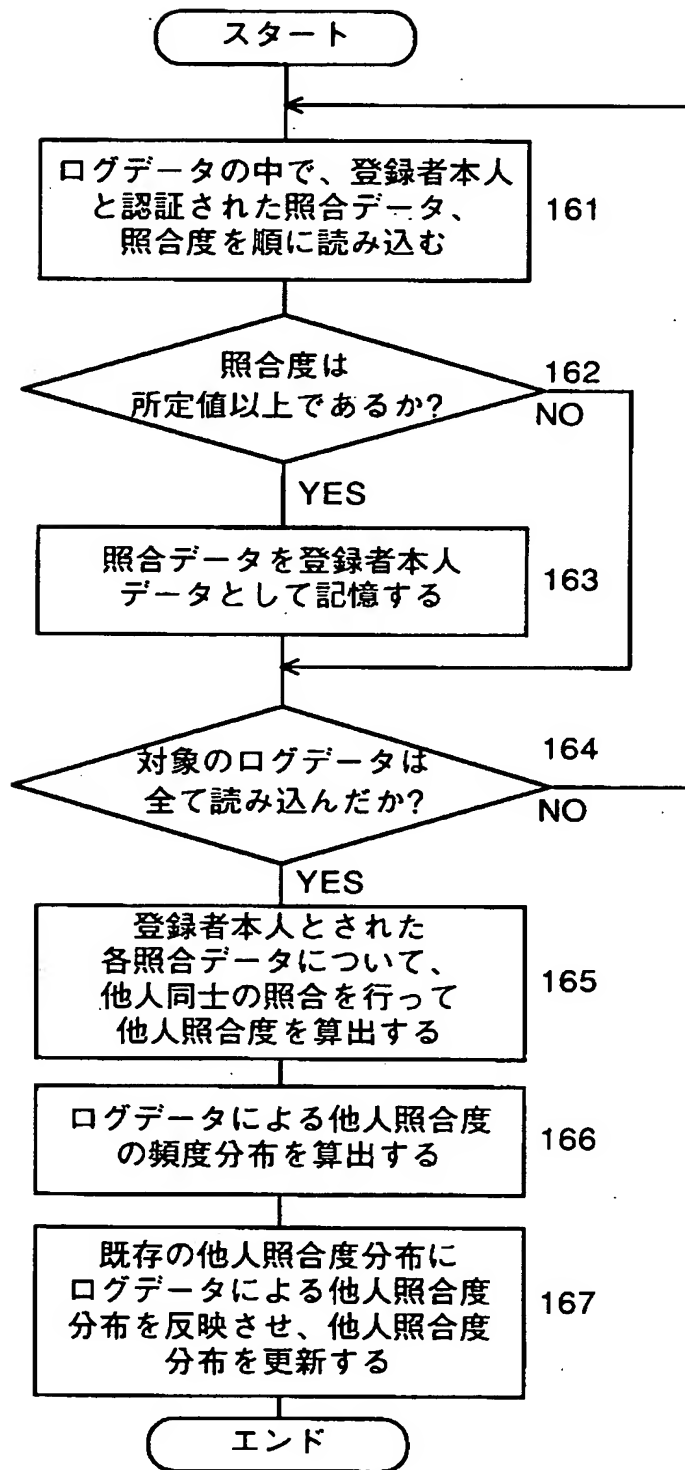




【図 12】



【図 13】



【図 1 4】

優先順位	認証手段の種類
1	指紋
2	虹彩
3	顔

【図 1 5】

認証の組合せ	指紋の照合度の 閾値 (T1)	虹彩の照合度の 閾値 (T2)
指紋AND指紋	60	—
指紋AND指紋AND虹彩	35	45
指紋AND指紋AND虹彩AND虹彩	35	40
指紋AND虹彩	55	50
指紋AND虹彩AND虹彩	40	40
虹彩AND虹彩	—	55
虹彩	—	50

【図 1 6】

優先順位	認証の組合せ方法
1	重み付き線形和
2	AND
3	OR

【書類名】            要約書

【要約】

【課題】    認証に要求される目標性能を満たす一の認証又は認証の組み合わせを選択する認証の選択システムを提供する。

【解決手段】    認証の選択システムは、被認証者を認証する少なくとも一つの認証手段を用いた認証に要求される目標性能を満たす、一の認証又は認証の組み合わせを選択する認証手段選択部 2 6 を備える。好ましくは、被認証者を認証する少なくとも一つの認証手段を用いた一の認証又は認証の組合せを生成する組合せ生成部 2 4 と、前記一の認証又は認証の組合せごとの認証性能を演算する複合認証性能演算部 2 5 とをさらに備える。認証システムは、上記認証の選択システムと、被認証者を認証する少なくとも一つの認証手段 1 1、1 2 とを備える。

【選択図】            図 1

出 願 人 履 歴 情 報

識別番号 [000006013]

1. 変更年月日	1990年 8月24日
[変更理由]	新規登録
住 所	東京都千代田区丸の内2丁目2番3号
氏 名	三菱電機株式会社